Access Manager Appliance 4.2 Release Notes

November 2015

Access Manager Appliance 4.2 includes new features, enhancements, improves usability, and resolves several previous issues.

Many of these improvements are made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure our products meet all your needs. You can post feedback in the Access Manager forum on our community website that also includes product notifications, blogs, and product user groups.

For information about the previous release, see Access Manager Appliance 4.1 SP1 Hotfix 1 Release Notes.

For more information about this release and for the latest release notes, see the Documentation page. To download this product, see the Product Upgrade page.

1 What’s New?

Access Manager Appliance 4.2 provides the following key features, enhancements, and fixes in this release:

NOTE: Platform Agent and Novell Audit are no longer supported. A new Access Manager 4.2 installation no longer installs Platform Agent and Novell Audit for auditing. If you upgrade from an older version of Access Manager to 4.2, Platform Agent is still available. It is recommended to use syslog for auditing.

1.1 New Features

This release introduces the following new features and enhancements:

1.1.1 Administration Console Dashboard

The Access Manager 4.2 release contains a redesigned Administration Console Dashboard. The Administration Console Dashboard retains the toolbar, so you can perform tasks as in previous versions of Access Manager. The new Administration Console Dashboard has the following advantages:

- You can view the health of various Access Manager components in the dashboard. If the component is healthy, the icons are green. If the component is not healthy, the icons are yellow or red.
- You can access common tasks easily through the dashboard. For example, you can quickly access:
  - Auditing
  - Certificates
  - Troubleshooting
  - Alerts
- You can expand and collapse the containers to view as much or as little as you want. For example, you can view the containers for the policies or you can view the containers and all of the policies in the container.
- The Access Manager components are displayed in a single view. You can expand the view and click any displayed component to launch the configuration page related to that component.

1.1.2 Mobile and Web Access

Access Manager 4.2 enables you to provide web and mobile access to protected applications and resources to your users easily through the MobileAccess feature. MobileAccess provides a configuration option in the Administration Console and an app for mobile devices.

MobileAccess contains appmarks, which are bookmarks for Access Manager resources. After you have configured an Access Manager resource, you configure one or more appmarks to enable users to access the resource in various ways.

Users can access the appmarks through the new user portal page or through the MobileAccess app on mobile devices. For more information, see Enabling Mobile and Web Access in the NetIQ Access Manager Appliance 4.2 Administration Guide.

1.1.3 New User Portal Page

This release introduces an enhanced portal where users log in to access resources protected by Access Manager. You can quickly set up the portal by creating **appmarks** that represent each protected resource. Appmarks function like a bookmark in a browser and provide secure access to the resources. As you create each appmark, the user portal immediately displays it. However, users can see only the appmarks that apply to their Access Manager roles.

You create the appmarks in the Administrative Console. You can also customize the branding in the user portal, such as your company logo and color theme.

This new user portal replaces the previous portal as the default login page for users. It supports both the features introduced in this release and the functionality available in the old user portal. If you prefer to maintain the customization that you previously created in JSP files, you can continue using the old portal after upgrading to this release. For more information about enabling your JSP files, see Customizing The Identity Server in the NetIQ Access Manager Appliance 4.2 Administration Guide.

NOTE: If you have customized the legacy user portal page and want to keep the customized pages, you must perform the steps mentioned under Maintaining Customized JSP Files for the Identity Server in the NetIQ Access Manager Appliance 4.2 Installation and Upgrade Guide.

1.1.4 Mobile Authentication SDK for iOS

To help you create custom iOS app to use with MobileAccess in Access Manager 4.2, NetIQ created a Mobile Authentication SDK for iOS. You can download the SDK from the NetIQ Access Manager Developer Tools and Examples website.

The SDK contains embedded documentation.

1.1.5 Administration REST APIs

This release provides REST APIs to automate the administration of Access Manager. These APIs are exposed by the Administration Console to allow the following common tasks to be handled automatically:

- Get the health of Identity Servers and Access Gateways
- Get the statistics Identity Servers and Access Gateways
- Refresh the metadata of the SAML2 trusted providers
- Renew certificates
- Get the active user sessions and terminate user sessions
- Purge Access Gateway cache
- Apply the configuration to the devices

The REST API guide is located on the NetIQ Access Manager Developer Tools and Examples website. This guide has information about all the REST APIs supported by Access Manager including OAuth APIs and device statistics APIs that were introduced in previous releases.

1.1.6 Risk-based Authentication Enhancements

Access Manager Appliance 4.2 provides the following enhancements in the risk-based authentication feature:

- **Intuitive Interface:** The new interface enables to configure all related entities such as risk policy, rule, risk levels, and risk-based authentication classes at one place. In Access Manager Appliance 4.2, a rule group is called as a risk policy.
- **New Approach to Configure Risk-Based Authentication:** In Access Manager Appliance 4.2, you can configure risk-based authentication to assess and mitigate risks before authenticating a login attempt. This option is in addition to the risk-based configuration after authenticating a login attempt.
- **New Privilege Rules:** In addition to **Allow Access**, Access Manager Appliance 4.2 provides a new privilege rule, **Deny Access**.
- **Rule Priority:** Rules are executed based on their priority. In Access Manager Appliance 4.2, you can change the priority of a rule by dragging and dropping the rule on the UI. The priority of rules decrease from top to bottom on the UI.
- **Score Sharing URLs:** Access Manager Appliance 4.2 enables you to send user name, risk score, and risk level of a specific login attempt to an external REST interface.
- **Enhanced Rule Validation Tool:** The rule validation tool has been enhanced and it now includes a graphical representation also.
- **Enhancement in the IP Rule:** Now, you can configure to fetch IP addresses by specifying the URL of a service provider.
- **Using External Parameters in Risk Assessment:** Access Manager Appliance 4.2 provides an option to consider inputs from external providers in evaluating the risk associated with a login attempt.
- **MS SQL support:** In addition to MYSQL and Oracle, Access Manager Appliance 4.2 supports the Microsoft SQL Server database for storing user history.
- **Cumulative Score:** Access Manager Appliance 4.2 provides an option to enable adding risk scores of the current session while evaluating a contract.
- **Risk Score Reduction after a Successful Additional Authentication:** Access Manager Appliance 4.2 provides an option to reduce the risk score by a specified value after a successful additional authentication.
- **Enhancement in Historical Entry Type:** The risk rule now considers user history from the database based on number of days instead of number of entries.
- **Statistics for Risk-Based Authentication:** The following statistics have been added:
  - Requests Allowed After Authentication
  - Requests Denied After Authentication
  - Requests Allowed Pre-Authentication
  - Requests Denied Pre-Authentication
  - Requests for Additional Authentication in Pre-Authentication
  - Requests for Additional Authentication in Post-Authentication

For more information, see “Risk-Based Authentication” and “Risk-Based Policies” in the *NetIQ Access Manager Appliance 4.2 Administration Guide*.

1.1.7 New Report on Risk Based Authentication

A new RBA report is included in Access Manager Reporting Solution Pack. This report provides the access count and details of action taken for risk-based authentication for individual applications.

For a sample report, see “Application Specific Risk based Authentication Report” in the *NetIQ Access Manager Appliance 4.2 Administration Guide*.

1.1.8 Attribute Retrieval and Transformation

With this release of Access Manager Appliance, you can retrieve an attribute from an external source and transform it before sending it in an assertion. The user attribute retrieval and transformation feature enables you to retrieve attributes from a data source (any database or LDAP repositories) and transform them. This feature also allows you to transform user’s local attributes (LDAP attributes, Shared Secrets, and various profiles such as Personal Profile and Employee Profile). For more information about user attribute retrieval and transformation, see User Attribute Retrieval and Transformation in the NetIQ Access Manager Appliance 4.2 Administration Guide.

1.1.9 Wizard-Based Configuration for Amazon Web Services

This release introduces an easy way to establish single-sign on with Amazon Web Services (AWS) on a federated setup. You can access this wizard in SAML 2.0 Service Provider configuration. Integration of AWS is simpler because most of the settings are pre-configured. For more information, see Integrating Amazon Web Services with Access Manager in the NetIQ Access Manager Appliance 4.2 Administration Guide.

1.1.10 Syslog Support and Audit Changes

Access Manager Appliance 4.2 now supports syslog for auditing. Syslog enables you to log audit events to a Sentinel server, Sentinel Log Manager, or a third party syslog server. For more information, see Configuring Access Manager Appliance for Auditing in the NetIQ Access Manager Appliance 4.2 Administration Guide.

The syslog events are logged by using the JSON format. For more information, see Access Manager Audit Events and Data in the NetIQ Access Manager Appliance 4.2 Administration Guide.

This release also introduces request-level audit filtering. For example, an Image filter excludes images from an audit event.

Access Manager no longer supports Platform Agent and Novell Audit for auditing.

1.1.11 User Interface for Configuring SAML Options

In addition to the UI support of some SAML options in the 4.1 release, this release enables you to configure all SAML options in the Administration Console. Configuring these options by using files is deprecated. For more information, see Defining Options for SAML 2.0 in the NetIQ Access Manager Appliance 4.2 Administration Guide.

1.1.12 User Interface for Configuring Identity Server Global Options

This release introduces a new UI for configuring Identity Server global options. Configuring these options by using files is deprecated. For more information about these properties, see Configuring Identity Server Global Options in the NetIQ Access Manager Appliance 4.2 Administration Guide.

1.1.13 User Interface for Configuring ESP Global Options

This release introduces a new UI for configuring ESP global options. Configuring these options by using files is deprecated. For more information about these properties, see Configuring ESP Global Options in the NetIQ Access Manager Appliance 4.2 Administration Guide.

1.1.14 User Interface for Configuring an Authentication Contract’s Options

You can configure an authentication contract to perform the following actions:

- To redirect a user trying to log in to the authentication contract with an expired password to the password management URI.
- To hide contracts with equal levels.

For more information, see Configuring Options for an Authentication Contract in the NetIQ Access Manager Appliance 4.2 Administration Guide.

1.2 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.6
- Java 1.8.0_66
- Apache 2.2.27 (This release includes fixes for CVE-2014-0231, CVE-2014-0226, CVE-2013-5704,and CVE-2015-3183)
- OpenSSL 1.0.1p
- Tomcat 8.0.24
- iManager 2.7.7.5

NOTE:

Access Manager 4.2 by default supports Tomcat 8.0.24 and OpenSSL 1.0.1p but the Administration Console uses Tomcat version 7.0.56 due to dependency on iManager.

1.3 Fixed Issues

This release includes software fixes for the following components:

- Section 1.3.1, “Identity Server,” on page 6
- Section 1.3.2, “Access Gateway,” on page 8

1.3.1 Identity Server

The following issues are fixed in the Identity Server component:

- Section 1.3.1.1, “Re-authentication Required During a spsend Request When Contract Contains the Equal or higher level Flag,” on page 7
- Section 1.3.1.2, “Only One Value of a Multi-Valued LDAP Attribute Is Available in the OAuth User Claims,” on page 7
- Section 1.3.1.3, “The User Profile Risk Rule Fails When the Selected Attribute of an LDAP User Is Multi-Valued,” on page 7

1.3.1.1 Re-authentication Required During a spsend Request When Contract Contains the Equal or higher level Flag

Issue: When a user is authenticated and step up authentication with **Equal or higher level** flag is executed, the Identity server prompts for re-authentication. This happens when a user is already authenticated with same level contract and if spSend step-up contract contains the **Equal or higher level** flag. [`Bug 945227`]

Fix: This issue is fixed. During step-up authentication, if the user is already authenticated with same level contract, re-authentication is not required.

1.3.1.2 Only One Value of a Multi-Valued LDAP Attribute Is Available in the OAuth User Claims

Issue: In the OAuth **User Claims**, the Identity Server displays only one value instead of displaying the multi-valued LDAP attribute. [`Bug 947305`]

Fix: This issue is resolved for custom claims. For example, you can add additional email field in **Custom claims** if multiple email is required. This is not applicable for openid connect standard predefined claims.

1.3.1.3 The User Profile Risk Rule Fails When the Selected Attribute of an LDAP User Is Multi-Valued

Issue: In a User Profile Risk rule, the rule evaluation fails when the selected LDAP user attribute is a multi-valued LDAP attribute such as, **memberof**, **and sn**.

Fix: This issue is now resolved. A User Profile Risk rule does not fail when the selected attribute of an LDAP user is multi-valued.

1.3.1.4 The User Profile Risk Rule Fails When the LDAP User Attribute Is Case-Sensitive

Issue: In a User profile Risk rule, the rule evaluation fails when the selected LDAP user attribute is case-sensitive. [`Bug 938385`]

Fix: This issue is resolved and the User Profile Risk rule does not fail when the LDAP user attribute is case-sensitive.

1.3.1.5 Attributes are Unavailable for an Embedded Service Provider in Transient Federation

Issue: In a transient federation, when an Embedded Service Provider (ESP) requests an attribute from the local identity provider over SAML federation, the attribute value is not retrieved from the remote identity provider. [`Bug 938531`]

Fix: This issue is resolved. In a transient federation, attribute cache initialization is performed during pre-authentication instead of post-authentication. Hence, the requested attribute is available for ESP.

1.3.1.6 Identity Provider Allows Unvalidated Redirects and Forwards

Issue: Identity Provider allows users to redirect to any set target without any validation of the URL that is set in the request. [`Bug 923078`]

Fix: This issue is resolved. The user interface is enhanced to define the valid whitelist application.

1.3.2 Access Gateway

The following issues are fixed in the Access Gateway:

- Section 1.3.2.1, “OAuth Claims Are Unavailable in an Identity Injection Policy,” on page 8
- Section 1.3.2.2, “The Access Gateway Statistics Report Incorrect Number of Connections to Origin Server,” on page 8
- Section 1.3.2.3, “Form Fill Corrupts Application Cookie When Cookie Mangling Is Enabled,” on page 8
- Section 1.3.2.4, “Host HTTP Header Attack,” on page 8
- Section 1.3.2.5, “Issue in Rewriting Location Header with the URL in the Query,” on page 8
- Section 1.3.2.6, “The Session Cache for POST Data Is Not Posted After Authentication or Re-authentication,” on page 8

1.3.2.1 OAuth Claims Are Unavailable in an Identity Injection Policy

Issue: In an Identity Injection policy, the Policy page does not display all OAuth claims configured in the resource server. [`Bug 947315`]

Fix: This issue is resolved and the Policy page displays all the available OAuth claims.

1.3.2.2 The Access Gateway Statistics Report Incorrect Number of Connections to Origin Server

Issue: When monitoring the Access Gateway statistics, the reports display incorrect value for number of connections to Origin Server. [`Bug 873699`]

Fix: This issue is fixed and the correct number of connections to Origin Server is displayed.

1.3.2.3 Form Fill Corrupts Application Cookie When Cookie Mangling Is Enabled

Issue: When cookie mangling is enabled, processing the Form Fill policy corrupts the application cookie. [`Bug 929810`]

Fix: This issue is fixed and application cookie does not get corrupt due to Form Fill when cookie mangling is enabled.

1.3.2.4 Host HTTP Header Attack

Issue: In the Access Gateway, a Host HTTP Header attack exists. An additional HTTP header is added with the original header. This header redirects you to a malicious URL. [`Bug 905262`]

Fix: This issue is resolved now as the Access Gateway in no longer susceptible to the host HTTP Header attack.

1.3.2.5 Issue in Rewriting Location Header with the URL in the Query

Issue: The Rewriter rewrites the location header with the URL in the query string automatically. There is no option to enable or disable rewriting the location header. [`Bug 915839`]

Fix: This issue is now resolved and the Rewriter rewrites the location header with the URL in the query string only when you enable the **RWOutboundHeaderQueryString** advance option. For more information about this option see Advanced Access Gateway Options in the NetIQ Access Manager Appliance 4.2 Administration Guide.

1.3.2.6 The Session Cache for POST Data Is Not Posted After Authentication or Re-authentication

Issue: During authentication or re-authentication, a new session cache is created without restoring the POST data and the data is lost.

Fix: This issue is fixed and now data is not lost and gets posted from the session cache after authentication or re-authentication.

2 Installing or Upgrading

After purchasing Access Manager Appliance 4.2, log in to the NetIQ Downloads page and follow the link that allows you to download the software. The following files are available:

Table 1 *Files Available for Access Manager Appliance 4.2*

Filename	Description
`AM_42_AccessManagerAppliance.iso`	Contains the Access Manager Appliance iso.
`AM_42_AccessManagerAppliance.tar.gz`	Contains the Access Manager Appliance tar file.

For information on the upgrade paths, see Section 3, “Supported Upgrade Paths,” on page 9. For more information about installing and upgrading, see the NetIQ Access Manager Appliance 4.2 Installation and Upgrade Guide.

3 Supported Upgrade Paths

To upgrade to Access Manager 4.2, you need to be on one of the following versions of Access Manager:

- 3.2.x
  - 3.2 Service Pack 3
  - 3.2 Service Pack 3 Hotfix 1
- 4.0.x
  - 4.0
  - 4.0 Hotfix 1
  - 4.0 Hotfix 2
  - 4.0 Hotfix 3
  - 4.0 Service Pack 2
  - 4.0 Service Pack 2 Hotfix1
- 4.1.x
  - 4.1
  - 4.1 Service Pack 1
  - 4.1 Service Pack 1 Hotfix 1

For more information about upgrading Access Manager Appliance, see “Upgrading Access Manager Appliance” in the *NetIQ Access Manager Appliance 4.2 Installation and Upgrade Guide*.

4 Verifying Version Number After Upgrading to 4.2

After upgrading to Access Manager 4.2, verify that the version number of the component is indicated as **4.2.0.0-221**. To verify the version number, perform the following steps:

1. In the Administration Console, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.2.0.0-221**.

5 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

5.1 Issue with Uninstalling the Secondary Administration Console

Issue: After the uninstallation of the secondary administration console fails, a message indicating that the process was successful is displayed. [`Bug 952073`]

Workaround: You must manually remove the information for the Administration Console. For more information, see the **Other Known Device Manager Servers** option under Checking for Potential Configuration Problems in the NetIQ Access Manager Appliance 4.2 Administration Guide.

5.2 Maintaining Customized JSP Files Requires Manual Steps

Issue: The upgrade process overwrites any customized `.jsp` files and the Access Manager Appliance 4.2 release requires manual steps to use any customized `.jsp` files.

Solution: You must perform manual steps for the NIDP and Access Gateway to maintain your customized `.jsp` files and have the new functionality in Access Manager Appliance. For more information, see Maintaining Customized JSP Files for the Identity Server and Maintaining Customized JSP Files for the Access Gateway in the NetIQ Access Manager Appliance 4.2 Installation and Upgrade Guide.

5.3 Delegated Administrators Cannot Access the New Panels of the Administration Console

Issue: The underlying architecture of Access Manager Appliance has changed in the Access Manager Appliance 4.2 release. These changes do not allow delegated administrators to access the new panels of the Administration Console. [`Bug 948692`]

Workaround: Delegated administrators can access resources through the toolbar.

5.4 MobileAccess App to an External Browser Can Time-out

Issue: If the users perform a service provider (SP)-initiated login from the MobileAccess app to an external browser, the session times out after 60 minutes. If the user is still using the application, the browser redirects them to the login screen.

Workaround: The user must login in again after the time-out has occurred.

5.5 The Administration Console Displays Deleted Devices

Issue: An administrator is using Internet Explorer or Edge to manage Access Manager Appliance. The administrator deletes a registered device through the MobileAccess feature. After deleting the device, the administrator access the dashboard and returns to view all registered devices. The Administration Console still lists the device as registered. [`Bug 952867`]

Workaround: Clear the cache on the Internet Explorer or Edge browser. You can also use a different browser.

5.6 The User Portal Does Not Display Configuration Changes for Branding

Issue: An administrator logs in to the secondary Administration Console and creates a new appmark or modifies the branding information. After clicking **Save**, the User Portal page does not display the new appmark or modified branding. [`Bug 947198`]

Solution: Ensure that you are connected to the primary Administration Console when creating appmarks or making any branding changes. Otherwise, make another change on the primary Administration Console or restart the IDPs.

5.7 Access Manager Appliance 4.2 Displays an Internal Error During Logout Request

Issue: When logout request is executed in a heavy load testing, Access Manager Appliance 4.2 displays `500 internal error` message on the server. [`Bug 929920`]

Workaround: There is no workaround.

5.8 The x509 Authentication Fails with Online Certificate Status Protocol Method of Verification

Issue: When the Content Length header is not set, or set to none in Online Certificate Status

Protocol (OCSP) response, the x509 certificate based authentication fails. [Bug 947182]

Workaround: There is no workaround.

5.9 Incorrect Reference to User Store When a Contract Uses the Same Class with Different Methods and LDAP Store

Issue: When two Kerberos contracts that use different methods and LDAP store, but use same class, the Identity Provider queries and fetches attributes from an incorrect user-store. [Bug 951372]

Workaround: There is no workaround.

5.10 The Rewriter Does Not Exclude DNS Names Specified in Exclude DNS Name List

Issue: The URL references containing excluded DNS names are rewritten even when the DNS names are specified in the **Exclude DNS Name List** option. [Bug 927855]

Fix: There is no workaround.

5.11 The Host Header Does Not Match with the Published DNS Name

Issue: When host header containing IP address does not match published DNS name or IP address and when the **Error on DNS mismatch** option is disabled, the request does not match with the parent proxy instead it matches with a different proxy.

Workaround: There is no workaround.

5.12 MobileAccess App Does Not Support Risk-based Authentication

Issue: When Risk-based authentication is configured, the mobile app does not evaluate the risk during registration. [Bug 954489]

Workaround: No workaround. However, MobileAccess allows you to specify which contract to use for authentication. You can choose a multi-factor authentication mechanism supported on a mobile (such as OTP and SMS).

6 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information Web site (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate Web site (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of Qmunity (http://community.netiq.com/), our community Web site that offers product forums, product notifications, blogs, and product user groups.

7 Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.